UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/653,227	08/31/2000	Bernard A. Traversat	5181-64800	4782

7590   10/04/2006

ROBERT C. KOWERT
CONLEY, ROSE & TAYON, P.C.
P.O. BOX 398
AUSTIN, TX 78767-0398

EXAMINER
CHEN, SHIN HON

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

UNITED STATES PATENT AND TRADEMARK OFFICE

MAILED

OCT n 4 2006

Technology Center 2100

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/653,227
Filing Date: August 31, 2000
Appellant(s): TRAVERSAT ET AL.

Robert C. Kowert
Reg. No. 39,255
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 4/24/06 appealing from the Office action mailed

10/18/05.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

a.   The rejection to claims 1-6, 8-31, 33-47, and 49-72 under judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-47 of co-pending Application No. 09/653,215 is withdrawn based on amendment to the co-pending Application No. 09/653,215.

b.   Claims 27, 28, 33-36, 38-43, 47, 49-51, 56-59, 61-63, 66, 67, 69, 70, and 72 stand finally rejected under 35 U.S.C. 102(a) as being anticipated by Adams.

c.   The rejection of Claims 29-31, 44, 45, 52, 53, 55, 64, and 65 stand finally rejected

35 U.S.C. 103(a) as being unpatentable over Adams in view of Czerwinski.

d.   New ground of rejection is applied to claims 62-72 under U.S.C 101.

NEW GROUND(S) OF REJECTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or
any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and
requirements of this title.

The claimed invention is directed to non-statutory subject matter. Claims 62-72

discloses a carrier medium and the carrier medium is described on page 146 of the

specification as transmission medium or signals.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,718,470   ADAMS   4-2004

Czerwinski, et al. "An Architecture for a Secure Service Discovery Service," Mobicom

99, Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing

and Networking, August 15th, 1999. XP000896069, pp 24-35.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis

for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1, 2, 8-13, 15-17, 20, 21, 23-26, 27, 28, 33-36, 38-43, 47, 49-51, 56-59, 61-63, 66, 67,

69, 70, and 72 are rejected under 35 U.S.C. 102(a) as being clearly anticipated by Adams

U.S. Pat. No. 6718470 (hereinafter Adams).

As per claim 1, Adams discloses a method for communicating in a distributed computing

environment, comprising: a client accessing an authentication service to obtain an authentication

credential to use a first service (Adams: column 6 lines 31-67: receiving the attribute certificate);

determining client capabilities for said client, wherein said client capabilities are capabilities of

said first service that said client is permitted to use (Adams: column 6 lines 49-61: the

centralized privilege data selector); binding said client capabilities to said authentication

credential (Adams: column 6 lines 65-66: the matching attributes are sent as pre-qualification

data); said client sending a first message to said first service, wherein said first message includes

said authentication credential (Adams: column 6 line 67 – column 7 line 8); said first service

using said authentication service to authenticate said authentication credential received in said

first message (Adams: column 7 lines 3-8: the relying party uses the centralized privilege data

selector to generate credential for authentication); and said first service responding to said first

message if said authentication credential in said first message is determined to be authentic as

from said client (Adams: column 7 lines 3-8).

As per claim 2, Adams discloses the method of claim 1. Adams further discloses the method

comprising said client obtaining an address for said authentication service from an advertisement

for said first service, wherein said accessing an authentication service comprises said client

sending a message to said address for said authentication service requesting said authentication

credential to use said advertised first service (Adams: figure 5 and column 5 lines 14-17 and

column 6 lines 44-52).

As per claim 8, Adams discloses the method of claim 1. Adams further discloses said client

sending a request message to said first service to access a capability of said first service, wherein

said request message includes said authentication credential (Adams: column 5 lines 13-18 and

column 6 line 67 – column 7 line 2); said first service determining that the capability requested

in said request message is within said client capabilities (Adams: column 7 lines 3-8); and said

first service fulfilling said request message only if the capability requested in said request

message is within said client capabilities (Adams: column 7 lines 3-8).

As per claim 9, Adams discloses the method of claim 1. Adams further discloses wherein said

determining client capabilities comprises said client accessing an access control policy service to

obtain a capability token indicating which capabilities of said first service said client permitted to access (Adams: column 6 lines 65-67).

As per claim 10, Adams discloses the method of claim 10. Adams further discloses wherein said authentication service and said access policy service are combined as a single service and wherein said capability token is included within said authentication credential (Adams: column 6 lines 31-67).

As per claim 11, Adams discloses the method of claim 1. Adams further discloses wherein said determining client capabilities is performed by said first service (Adams: column 6 lines 17-20: send the privilege test criteria data; column 7 lines 3-7: check the pre-qualification privilege data).

As per claim 12, Adams discloses the method of claim 1. Adams further discloses said client generating a message gate for accessing said first service, wherein said message gate sends request message from said client to said first service to access said first service, and wherein said message gate includes said authentication credential in each message to said first service (Adams: column 6 line 67 – column 7 line 8).

As per claim 13, Adams discloses the method of claim 1. Adams further discloses said client obtaining a service advertisement for said first service before accessing said first service,

wherein said service advertisement comprises an address for said authentication service and an address for said first service (Adams: column 5 lines 14-18 and column 6 lines 49-51).

As per claim 15, Adams discloses the method of claim 1. Adams further discloses wherein said authentication service is a separately addressable service from said first service (Adams: column 6 lines 38-42 and figure 5: centralized privilege data selector).

As per claim 16, Adams discloses the method of clam 1. Adams further discloses wherein said client accessing an authentication service to obtain an authentication credential to use a first service comprises said authentication service returning said authentication credential to said client only if said client is authorized to access said first service (Adams: column 6 lines 61-67: only send the matching attributes certificates).

As per claim 17, Adams discloses a method for communication in a distributed computing environment, comprising: a client obtaining a service advertisement for a first service, wherein said service advertisement includes an address for an authentication service (Adams: column 5 lines 13-18 and column 6 lines 49-52); said client sending a request message to said authentication service to obtain an authentication credential to use said first service (Adams: column 6 lines 49-52); said client generating a message gate for accessing said first service, wherein said message gate embeds said authentication credential in every message from said client to said first service (Adams: column 6 lines 65-67); and said client accessing said first service through said message gate (Adams: column 6 line 67 – column 7 line 8).

As per claim 20, Adams discloses the method of claim 17. Adams further discloses said first

service using said authentication service to determine if said authentication credential received in

a first message from said client is authentic (Adams: column 7 lines 3-8).

As per claim 21, Adams discloses the method of claim 20. Adams further discloses

authenticating said authentication credential received in said first message from said client, said

first service determining which capabilities of said first service said client is authorized to use,

wherein said first service responds to a request message from said client only if said request

message is for an authorized capability for said client (Adams: column 7 lines 3-8).

As per claim 23, Adams discloses the method of claim 20. Adams discloses said first service

noting whether or not said authentication credential is authentic so that said first service does not

need to repeat said using said authentication service to determine if said authentication credential

received in a first message from said client is authentic (Adams: column 5 lines 13-18).

Furthermore, Single-Sign-On is well known in the art to reduce the burden of authentication

services.

As per claim 24, Adams discloses the method of claim 17. Adams further discloses wherein said

service advertisement for said first service further includes an address for accessing said first

service, wherein said authentication service and said first service are separate services within the

distributed computing environment (Adams: column 5 lines 13-18 and column 6 lines 31-41).

As per claim 25, Adams discloses the method of claim 17. Adams further discloses wherein said

service advertisement further includes a service identifier token for said first service, wherein

said client sending a request message to said authentication service to obtain an authentication

credential comprises sending said service identifier token and a client identifier token to said

authentication service (Adams: column 6 lines 49-61).

As per claim 26, Adams discloses the method of claim 25. Adams further discloses wherein said

authentication service generates said authentication credential from said client identifier token

and said service identifier token (Adams: column 6 lines 49-61).

As per claim 27, 28, 33-36, 38-43, 47, 49-51, 56-59, 61-63, 66, 67, 69, 70, and 72 encompass the

same scope as claims 1, 2, 8-13, 15-17, 20, 21, and 23-26. Therefore, claims 227, 28, 33-36, 38-

43, 47, 49-51, 56-59, 61-63, 66, 67, 69, 70, and 72 are rejected based on the same reasons set

forth in rejecting claims 1, 2, 8-13, 15-17, 20, 21, and 23-26.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

Claims 3-6, 18, 19, 29-31, 44-45, 52, 53, 55, 64, and 65 are rejected under 35 U.S.C. 103(a)

as being unpatentable over Adams in view of Czerwinski et al. "An Architecture for a

Secure Service Discovery Service" (hereinafter Czerwinski).

As per claim 3, Adams discloses the method of claims 2. Adams does not explicitly disclose said

advertisement for said first service includes a data representation language schema defining a

message interface for accessing said first service. However, Czerwinski discloses defining a

message interface using XML for accessing a service (Czerwinski: 2.3 XML Service

Descriptions). It would have been obvious to use XML message interface to allow

communications between the relying parties and subscribers. Therefore, it would have been

obvious to one having ordinary skill in the art at the time of applicant's invention to combine the

teachings of Czerwinski within the system of Adams because XML is well known in the art to

provide greater flexibility as communication interfaces.

As per claim 4, Adams as modified discloses the method of claim 3. Adams as modified further

discloses wherein said first message corresponds to a message defined in said data representation

language schema(Czerwinski: 2.3: XML queries and 3.1 page 27 left column 5th paragraph).

As per claim 5, Adams as modified discloses the method of claim 4. Adams as modified further

discloses the method comprising said client sending additional messages to said first service to

use said first service, wherein said authentication credential is included with each one of said

additional messages (Adams: column 6 lines 31-67), and wherein each one of said additional

messages is defined by said data representation schema (Czerwinski: 2.3: XML queries).

As per claim 6, Adams as modified discloses the method of claim 5. Adams as modified further

discloses said data representation language schema is an eXtensible Markup Language (XML)

schema (Czerwinski: 2.3 XML Service Descriptions).

As per claim 18, Adams discloses the method of claim 17. Adams does not explicitly disclose

wherein said service advertisement further comprises a data representation language schema

defining a message interface for accessing said first service, the method further comprising said

message gate verifying that every message sent from said client to said first service complies

with said data representation language schema. However, Czerwinski discloses defining a

message interface using XML for accessing a service (Czerwinski: 2.3 XML Service

Descriptions). It would have been obvious to one having ordinary skill in the art at the time of

applicant's invention to use XML to communicate between two parties. Therefore, it would have

been obvious to one having ordinary skill in the art at the time of applicant's invention to

combine the teachings of Czerwinski within the system of Adams because XML allows the

encoding of arbitrary structures of hierarchical named values.

As per claim 19, Adams as modified discloses the method of claim 18. Adams as modified

further discloses wherein said data representation language schema is an eXtensible Markup

Language (XML) schema and said messages from said client to said first service are XML

messages (Czerwinski: 2.3 XML Service Descriptions).

As per claim 29-31, 44, 45, 52, 53, 55, 64, and 65, claims 29-31, 44, 45, 52, 53, 55, 64, and 65

encompass the same scope as claims 3-6, 18, and 19. Therefore, claims 29-31, 44, 45, 52, 53, 55,

64, and 65 are rejected based on the same reasons set forth in rejecting claims 3-6, 18, and 19.

(10) Response to Argument

1.   **Claims 1, 2, 8-13, 15-17, 20, 21, and 23-26 stand finally rejected under 35 U.S.C**

102(a) as being anticipated by Adams (U.S. Pat. 6,718,470).

Claims 1, 8, 15, and 16:

Regarding Claim 1, Appellants argue Adams fails to disclose determining client

capabilities for a client; binding the client capabilities to the authentication credential; and

using the authentication service to authenticate the authentication credential.

Examiner respectfully disagrees. Adams clearly discloses determining client capabilities

for a client (Adams: column 6 lines 52-55 and 58-60: the centralized privilege data selector

obtains the attributes certificate of subscribers from attributes certificate repository according to

subscriber's identification data). The centralized privilege data selector determines the

capabilities of subscriber by using the subscriber's identification data to retrieve attribute

certificate associated with the subscriber. Adams also discloses binding the client capabilities to

the authentication credential (Adams: column 6 line 65 – column 7 line 2: the matching attributes

certificates are sent as pre-qualification data). The capabilities/attribute certificates of client are

sent to clients in form of pre-qualification privilege data/authentication credential. Lastly, Adams

discloses using the authentication service to authenticate the authentication credential (Adams:

column 6 line 61 – column 7 line 9: the pre-qualification privilege data). The pre-qualification

privilege data is generated by the authentication service/centralized privilege data selector so that

it can be verified by the first service/relying party, thus the first service uses the authentication

service to authenticate subscribers based prior to grant access to subscribers. Therefore, Adams

discloses all the limitations of claim 1.

Claim 2:

Regarding Claim 2, Appellants argue Adams fails to disclose a client obtaining an

address for the authentication service <u>from an advertisement for the service</u>.

Examiner respectfully disagrees. Adams discloses that the subscriber requests access to

the service through a Website and the subscriber provides the identification of the service and

subscriber to the authentication service (Adams: column 5 lines 14-17: Website of relying party;

column 6 lines 49-51: the identification of relying party and subscriber). Therefore, in order for

the subscriber to request authentication credential, the subscriber must be informed of the

authentication service's address.

Claim 9:

Regarding Claim 9, Appellants argue Adams does not disclose that determining a

client capabilities includes the client accessing the access policy service to obtain a

capability token <u>indicating which capabilities of the service the client is permitted to access</u>.

Examiner respectfully disagrees. Adams discloses that the subscribers obtains the pre-

qualification privilege data from centralized privilege data selector and the pre-qualification

privilege data includes attribute certificates that the subscriber associated with (Adams: column 6 lines 65-67 and column 6 line 53-55: subscriber attribute certificate repository). Although the terms used by Appellants and Adams are not identical, the terms can be interchangeably used. Therefore, the pre-qualification privilege data includes the capabilities of the service that the subscriber is permitted to access.

Claim 10:

Regarding Claim 10, Appellants argue Adams fails to disclose an authentication service and an access policy service that are <u>combined as a single service and where the capability token is included within the authentication credential.</u>

Examiner respectfully disagrees. Adams discloses that the subscriber attribute certificate repository and the centralized privilege data selector are combined as a single service to provide authentication credential to subscribers (Adams: column 6 lines 53-67). The access policy service and the authentication service combined as a single service in the form of subscriber attribute certificate repository and centralized privilege data selector. Therefore, Adams clearly discloses the limitation of claim 10.

Claim 11:

Regarding Claim 11, Appellants argue Adams fails to disclose where determining client capabilities is <u>performed by the service.</u>

Examiner respectfully disagrees. Adams discloses that the relying party/first service checks the pre-qualification privilege data to ensure if the subscriber is authorized to access the service (Adams: column 7 lines 3-7). Therefore, the relying party determines what the subscriber is authorized to access prior to granting access.

Claim 12:

Regarding Claim 12, Appellants argue Adams fails to disclose the client __generating__ __a message gate__ for accessing the service and where the message gate __includes the__ __authentication credential in each message to the first service.__

Examiner respectfully disagrees. Adams discloses that the pre-qualification privilege data is sent with access request to relying party through suitable communication link and a communication system employing cryptography based security (Adams: column 4 lines 10-11: cryptography based security; and column 6 line 67- column 7 line 2: suitable communication link). Since the communication is encrypted and the pre-qualification privilege data transmitted to relying party when requesting a service, thus a message gate is generated and the authentication credential in included in each message to the first service.

Claim 13:

Regarding Claim 13, Appellants argue Adams fails to disclose the client __obtaining a__ __service advertisement for the first service__ before accessing the first service, where the service advertisement __includes an address for the authentication service and an address for__ __the first service.__

Examiner respectfully disagrees. Adams discloses that the subscriber requests access to the service through a Website and the subscriber provides the identification of the service and subscriber to the authentication service (Adams: column 5 lines 14-17: Website of relying party; column 6 lines 49-51: the identification of relying party and subscriber). Therefore, in order for the subscriber to request authentication credential, the subscriber must be informed of the authentication service's address as well as the first service's address.

Claims 17, 25, and 26:

Regarding Claim 17, Appellants argue Adams fails to disclose the client <u>obtaining a</u>
<u>service advertisement for the first service</u> before accessing the first service, where the
service advertisement <u>includes an address for the authentication service and an address for</u>
<u>the first service;</u> and <u>generating a message gate</u> for accessing the service and where the
message gate <u>includes the authentication credential in each message to the first service.</u>

Examiner respectfully disagrees. Adams discloses that the subscriber requests access to
the service through a Website and the subscriber provides the identification of the service and
subscriber to the authentication service (Adams: column 5 lines 14-17: Website of relying party;
column 6 lines 49-51: the identification of relying party and subscriber). Therefore, in order for
the subscriber to request authentication credential, the subscriber must be informed of the
authentication service's address as well as the first service's address. Furthermore, Adams
discloses that the pre-qualification privilege data is sent with access request to relying party
through suitable communication link and a communication system employing cryptography
based security (Adams: column 4 lines 10-11: cryptography based security; and column 6 line
67- column 7 line 2: suitable communication link). Since the communication is encrypted and
the pre-qualification privilege data transmitted to relying party when requesting a service, thus a
message gate is generated and the authentication credential in included in each message to the
first service.

Claim 20:

Regarding Claim 20, Appellants argue Adams fails to disclose <u>using the</u>
<u>authentication service to authenticate the authentication credential.</u>

Examiner respectfully disagrees. Adams clearly discloses using the authentication service

to authenticate the authentication credential (Adams: column 6 line 61 – column 7 line 9: the pre-

qualification privilege data). The pre-qualification privilege data is generated by the

authentication service/centralized privilege data selector so that it can be verified by the first

service/relying party, thus the first service uses the authentication service to authenticate

subscribers based prior to grant access to subscribers. Therefore, Adams discloses all the

limitations of claim 20.

Claim 21:

Regarding Claim 21, Appellants argue Adams fails to disclose where the first service

responds to a request message from the client <u>only if the request message is for an</u>

<u>authorized capability for the client.</u>

Examiner respectfully disagrees. Adams discloses that the relying party responds/grants

access to the request only if the pre-qualification privilege data contains proper attribute

certificates (Adams: column 7 lines 3-8). The definition of "responds" interpreted by the

examiner is when access is granted. Therefore, Adams clearly discloses that the request is

responded only if the subscriber obtains credentials enabling him/her to access service.

Claim 23:

Regarding Claim 23, Appellants argues that the rejection of claim 23 is improper.

Examiner respectfully disagrees. Adams discloses that a subscriber may communicate a

request over a global network link to a website of the relying party requesting access to another

application controlled by the relying party (Adams: column 5 lines 13-18). Adams might not

have explicitly disclosed the limitation of claim 23, but Adams inherently discloses that the

Single-Sign-On can be applied for services controlled by the same relying party. Therefore, the

rejection is proper.

Claim 24:

Regarding Claim 24, Appellants argue Adams fails to disclose where the service

advertisement includes an address for the authentication service and an address for the

first service.

Examiner respectfully disagrees. Adams discloses that the subscriber requests access to

the service through a Website and the subscriber provides the identification of the service and

subscriber to the authentication service (Adams: column 5 lines 14-17: Website of relying party;

column 6 lines 49-51: the identification of relying party and subscriber). Therefore, in order for

the subscriber to request authentication credential, the subscriber must be informed of the

authentication service's address as well as the first service's address.

2.   **Claims 3-6, 18, and 19 stand finally rejected under 35 U.S.C. 103(a) as being**

unpatentable over Adams in view of Czerwinski et al. "An Architecture for a Secure

Service Discovery Service".

Claim 3:

Regarding Claim 3, Appellants argue Adams in view of Czerwinski fails to teach or

suggest that the advertisement for the first service includes a data representation language

schema defining a message interface for accessing the first service.

Examiner respectfully disagrees. Adams discloses the subscriber access the relying party

service through website (Adams: column 5 lines 13-18). Adams does not disclose the first

service includes a data representation language schema defining a message interface for

accessing the first service. However, Examiner relies on Czerwinski to disclose service using

XML format to describer service descriptions and *client queries* (Czerwinski: 2.3). Therefore,

Czerwinski suggests that XML format can be used for service description and client queries to

establish interface between client and service.

Claim 4:

Regarding Claim 4, Appellants argue Adams in view of Czerwinski fails to disclose

that the first message, sent from the client to the service and including the authentication

credential, <u>corresponds to a message defined in the data representation language schema</u>.

Examiner respectfully disagrees. Czerwinski discloses that the XML format service

description and client queries are used for communication between client and service

(Czerwinski: 2.3 and 3.1). Therefore, Czerwinski suggests that XML format can be used for

service description and client queries to establish interface between client and service.

Claims 5 and 6:

Regarding Claims 5 and 6, Appellants argue Adams in view of Czerwinski fails to

teach or suggest the client sending additional messages to the service wherein the

<u>authentication credential is included with each one of the additional messages</u>; and

<u>additional messages are defined in the data representation language schema</u>..

Examiner respectfully disagrees. Adams discloses that the relying party checks the pre-

qualification privilege data prior to granting privilege to the subscriber (Adams: column 7 lines

5-9). The relying party checks the pre-qualification privilege data every time the subscriber

requests access, thus the authentication credential is included with each one of the additional

messages. Appellants further argue that Czerwinski does not disclose the limitation. However,

Czerwinski is not relied upon to disclose authentication credential is included with each one of

the additional messages. Furthermore, Appellants argue Czerwinski does not disclose addional

messages are defined in the data representation language schema. However, Czerwinski

discloses that the XML format service description and client queries are used for communication

between client and service (Czerwinski: 2.3 and 3.1). Therefore, Czerwinski suggests that XML

format can be used for service description and client queries to establish interface between client

and service.

Claims 18 and 19:

Regarding Claims 18 and 19, Appellants argue Czerwinski does not disclose that the

advertisement for the first service includes <u>a data representation language schema defining</u>

<u>a message interface for accessing</u> the first service; and the message gate <u>verifies that each</u>

<u>message sent from the client to the first service complies with the data representation</u>

<u>language schema</u>.

Examiner respectfully disagrees. Adams discloses the subscriber access the relying party

service through website (Adams: column 5 lines 13-18). Adams does not disclose the first

service includes a data representation language schema defining a message interface for

accessing the first service. However, Examiner relies on Czerwinski to disclose service using

XML format to describer service descriptions and *client queries* (Czerwinski: 2.3). Therefore,

Czerwinski suggests that XML format can be used for service description and client queries to

establish interface between client and service. Furthermore, Czerwinski discloses the message

gate verifies that the messages are in proper format prior to processing requests (Czerwinski: 2.3:

use XML format for client queries; page 27 left column 5th paragraph: the query is in the form of

XML). The queries need to comply with the format used by the service so that the service can

process query submitted by the client.

3.   **Claims 27, 28, 33-36, 38-43, 47, 49-51, 56-59, 61-63, 66, 67, 69, 70, and 72 stand**

finally rejected under 35 U.S.C. 102(a) as being anticipated by Adams.

        <u>Claims 27, 33, 38, 39, 41, and 42:</u>

        Regarding Claim 27, Appellants argue Adams fails to disclose <u>determining client</u>

<u>capabilities for a client; binding the client capabilities to the authentication credential; and</u>

<u>using the authentication service to authenticate the authentication credential.</u>

        Examiner respectfully disagrees. Adams clearly discloses determining client capabilities

for a client (Adams: column 6 lines 52-55 and 58-60: the centralized privilege data selector

obtains the attributes certificate of subscribers from attributes certificate repository according to

subscriber's identification data). The centralized privilege data selector determines the

capabilities of subscriber by using the subscriber's identification data to retrieve attribute

certificate associated with the subscriber. Adams also discloses binding the client capabilities to

the authentication credential (Adams: column 6 line 65 – column 7 line 2: the matching attributes

certificates are sent as pre-qualification data). The capabilities/attribute certificates of client are

sent to clients in form of pre-qualification privilege data/authentication credential. Lastly, Adams

discloses using the authentication service to authenticate the authentication credential (Adams:

column 6 line 61 – column 7 line 9: the pre-qualification privilege data). The pre-qualification

privilege data is generated by the authentication service/centralized privilege data selector so that

it can be verified by the first service/relying party, thus the first service uses the authentication

service to authenticate subscribers based prior to grant access to subscribers. Therefore, Adams

discloses all the limitations of claim 27.

Claim 28

Please refer to the responses above regarding the 102 rejection of claim 2 as they also

apply to claim 28.

Claim 34:

Please refer to the responses above regarding the 102 rejection of claim 9 as they also

apply to claim 34.

Claim 35:

Please refer to the responses above regarding the 102 rejection of claim 10 as they also

apply to claim 35.

Claim 36:

Please refer to the responses above regarding the 102 rejection of claim 12 as they also

apply to claim 36.

Claim 40:

Appellants argue that the 102 rejection is improper because the Examiner has failed

to provide a prima facie rejection.

Examiner respectfully disagrees, Adams discloses the client device is configured to

couple to a network via a wireless connection (Adams: column 7 lines 1-2). The communication

link incorporates any well known communication method including wireless connection.

Therefore, Appellants' argument is respectfully traversed.

Claims 43, 47, 49, and 50:

Regarding Claim 43, <u>determining client capabilities for a client; binding the client capabilities to the authentication credential; and using the authentication service to authenticate the authentication credential.</u>

Examiner respectfully disagrees. Adams clearly discloses determining client capabilities for a client (Adams: column 6 lines 52-55 and 58-60: the centralized privilege data selector obtains the attributes certificate of subscribers from attributes certificate repository according to subscriber's identification data). The centralized privilege data selector determines the capabilities of subscriber by using the subscriber's identification data to retrieve attribute certificate associated with the subscriber. Adams also discloses binding the client capabilities to the authentication credential (Adams: column 6 line 65 – column 7 line 2: the matching attributes certificates are sent as pre-qualification data). The capabilities/attribute certificates of client are sent to clients in form of pre-qualification privilege data/authentication credential. Lastly, Adams discloses using the authentication service to authenticate the authentication credential (Adams: column 6 line 61 – column 7 line 9: the pre-qualification privilege data). The pre-qualification privilege data is generated by the authentication service/centralized privilege data selector so that it can be verified by the first service/relying party, thus the first service uses the authentication service to authenticate subscribers based prior to grant access to subscribers. Therefore, Adams discloses all the limitations of claim 43.

Claims 51, 56, and 57:

Regarding Claim 51, <u>determining client capabilities for a client; binding the client</u>

<u>capabilities to the authentication credential;</u> and <u>using the authentication service to</u>

<u>authenticate the authentication credential.</u>

Examiner respectfully disagrees. Adams clearly discloses determining client capabilities

for a client (Adams: column 6 lines 52-55 and 58-60: the centralized privilege data selector

obtains the attributes certificate of subscribers from attributes certificate repository according to

subscriber's identification data). The centralized privilege data selector determines the

capabilities of subscriber by using the subscriber's identification data to retrieve attribute

certificate associated with the subscriber. Adams also discloses binding the client capabilities to

the authentication credential (Adams: column 6 line 65 – column 7 line 2: the matching attributes

certificates are sent as pre-qualification data). The capabilities/attribute certificates of client are

sent to clients in form of pre-qualification privilege data/authentication credential. Lastly, Adams

discloses using the authentication service to authenticate the authentication credential (Adams:

column 6 line 61 – column 7 line 9: the pre-qualification privilege data). The pre-qualification

privilege data is generated by the authentication service/centralized privilege data selector so that

it can be verified by the first service/relying party, thus the first service uses the authentication

service to authenticate subscribers based prior to grant access to subscribers. Therefore, Adams

discloses all the limitations of claim 51.

<u>Claim 58:</u>

Regarding Claim 58, Appellants argue Adams fails to disclose the client <u>obtaining a</u>

<u>service advertisement for the first service</u> before accessing the first service, where the

service advertisement <u>includes an address for the authentication service and an address for</u>

the first service; and generating a message gate for accessing the service and where the

message gate includes the authentication credential in each message to the first service.

Examiner respectfully disagrees. Adams discloses that the subscriber requests access to

the service through a Website and the subscriber provides the identification of the service and

subscriber to the authentication service (Adams: column 5 lines 14-17: Website of relying party;

column 6 lines 49-51: the identification of relying party and subscriber). Therefore, in order for

the subscriber to request authentication credential, the subscriber must be informed of the

authentication service's address as well as the first service's address. Furthermore, Adams

discloses that the pre-qualification privilege data is sent with access request to relying party

through suitable communication link and a communication system employing cryptography

based security (Adams: column 4 lines 10-11: cryptography based security; and column 6 line

67- column 7 line 2: suitable communication link). Since the communication is encrypted and

the pre-qualification privilege data transmitted to relying party when requesting a service, thus a

message gate is generated and the authentication credential in included in each message to the

first service.

Claim 59:

Please refer to the responses above regarding the 102 rejection of claim 18 as they also

apply to claim 59.

Claim 61:

Appellants argue Adams fails to disclose using the authentication service to

authenticate the authentication credential; and where the first service responds to a request

message from the client <u>only if the request message is for an authorized capability for the</u>

<u>client</u>.

Examiner respectfully disagrees. Adams clearly discloses using the authentication service

to authenticate the authentication credential (Adams: column 6 line 61 – column 7 line 9: the pre-

qualification privilege data). The pre-qualification privilege data is generated by the

authentication service/centralized privilege data selector so that it can be verified by the first

service/relying party, thus the first service uses the authentication service to authenticate

subscribers based prior to grant access to subscribers. Therefore, Adams discloses all the

limitations of claim 20. Furthermore, Adams discloses that the relying party responds/grants

access to the request only if the pre-qualification privilege data contains proper attribute

certificates (Adams: column 7 lines 3-8). The definition of "responds" interpreted by the

examiner is when access is granted. Therefore, Adams clearly discloses that the request is

responded only if the subscriber obtains credentials enabling him/her to access service.

Claim 62 and 66:

Please refer to the responses above regarding the 102 rejection of claim 1 as they also

apply to claims 62 and 66.

Claim 63:

Please refer to the responses above regarding the 102 rejection of claim 2 as they also

apply to claim 63.

Claim 67:

Please refer to the responses above regarding the 102 rejection of claim 12 as they also

apply to claim 67.

Claim 69:

Please refer to the responses above regarding the 102 rejection of claim 17 as they also apply to claim 69.

Claim 70:

Please refer to the responses above regarding the 102 rejection of claim 18 as they also apply to claim 70.

Claim 63:

Please refer to the responses above regarding the 102 rejection of claim 61 as they also apply to claim 72.

4.   **Claims 29-31, 44, 45, 52, 53, 55, 64, and 65 stand finally rejected 35 U.S.C. 103(a) as being unpatentable over Adams in view of Czerwinski.**

Claims 29 and 31:

Please refer to the responses above regarding the 103 rejection of claims 3 and 4 as they also apply to claims 29 and 31 respectively.

Claim 30:

Please refer to the responses above regarding the 102 rejection of claim 5 as they also apply to claim 30.

Claim 44:

Please refer to the responses above regarding the 103 rejection of claim 3 as they also apply to claim 44.

Claim 45:

Please refer to the responses above regarding the 103 rejection of claim 4 as they also

apply to claim 45.

Claim 52:

Please refer to the responses above regarding the 103 rejection of claim 3 as they also

apply to claim 52.

Claim 53 and 55:

Please refer to the responses above regarding the 103 rejection of claims 3 and 4 as they

also apply to claim 53 and 55.

Claims 64 and 65:

Please refer to the responses above regarding the 103 rejection of claims 3 and 4 as they also

apply to claims 64 and 65.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related

Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

This examiner's answer contains a new ground of rejection set forth in section **(9)** above.

Accordingly, appellant must within **TWO MONTHS** from the date of this answer exercise one

of the following two options to avoid *sua sponte* **dismissal of the appeal** as to the claims subject

to the new ground of rejection:

(1) **Reopen prosecution.** Request that prosecution be reopened before the primary

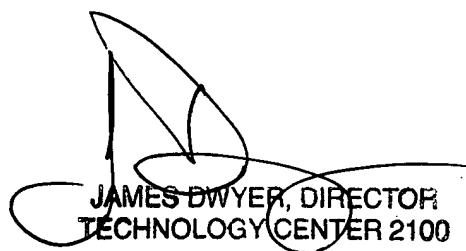examiner by filing a reply under 37 CFR 1.111 with or without amendment, affidavit or other

evidence. Any amendment, affidavit or other evidence must be relevant to the new grounds of

rejection. A request that complies with 37 CFR 41.39(b)(1) will be entered and considered. Any

request that prosecution be reopened will be treated as a request to withdraw the appeal.

(2) **Maintain appeal.** Request that the appeal be maintained by filing a reply brief as set

forth in 37 CFR 41.41. Such a reply brief must address each new ground of rejection as set forth

in 37 CFR 41.37(c)(1)(vii) and should be in compliance with the other requirements of 37 CFR

41.37(c). If a reply brief filed pursuant to 37 CFR 41.39(b)(2) is accompanied by any

amendment, affidavit or other evidence, it shall be treated as a request that prosecution be

reopened before the primary examiner under 37 CFR 41.39(b)(1).

Extensions of time under 37 CFR 1.136(a) are not applicable to the TWO MONTH time

period set forth above. See 37 CFR 1.136(b) for extensions of time to reply for patent

applications and 37 CFR 1.550(c) for extensions of time to reply for ex parte reexamination

proceedings.

Respectfully submitted,

Shin-Hon Chen

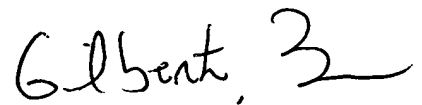JAMES DWYER, DIRECTOR
TECHNOLOGY CENTER 2100

A Technology Center Director or designee must personally approve the new

ground(s) of rejection set forth in section (9) above by signing below:

Conferees:

Gilberto Barron

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Kambiz Zand